(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 644 474 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **94306679.5**

(51) Int. Cl.[6] : **G06F 1/00,** G11B 20/00

(22) Date of filing : **12.09.94**

(30) Priority : **13.09.93 US 120969**

(43) Date of publication of application :
22.03.95 Bulletin 95/12

(84) Designated Contracting States :
DE GB

(71) Applicant : **NATIONAL UNIVERSITY OF SINGAPORE**
Heng Mui Keng Terrace,
Kent Ridge
Singapore 0511 (SG)

(72) Inventor : **Arcot Desai, Narasimhalu**
9 Ross Avenue
Singapore 1129 (SG)
Inventor : **Wang, Weiguo**
103 Jalan Hitam Manis
Singapore 1027 (SG)
Inventor : **Kankanhalli, Mohan Shankara**
74 Jalan Hitam Manis
Singapore 1027 (SG)

(74) Representative : **Driver, Virginia Rozanne et al**
Page White & Farrer
54 Doughty Street
London WC1N 2LS (GB)

(54) A method for utilising medium nonuniformities to minimize unauthorized duplication of digital information.

(57) The present invention is a method for preventing unauthorized copying and use of information which is stored on a storage medium and for restricting the use of such information to designated devices. Copy protection is achieved by generating a signature from a given storage medium. The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes. The selected list may contain nonuniformities at any granularity level. As such, this signature is unique to a given storage medium in the same way finger prints are unique to a human being. This signature is used to derive a key for encrypting the information on the storage medium. Any copying of the distribution information from one storage medium to another results in the mutation of the signature required to decrypt the information. Therefore, the present invention obviates the need for introducing artificial indica or requiring a special hardware subsystem for achieving a copy protection scheme.

Restricting the usage of information on a distribution medium to a designated device is achieved by verifying the device ID (DID-D) of the device with the device ID (DID-S) stored in the distribution medium before the decryption and transfer of information are undertaken. Decryption of the information is accomplished by generating a key from both the signature of the distribution medium and the DID-S.

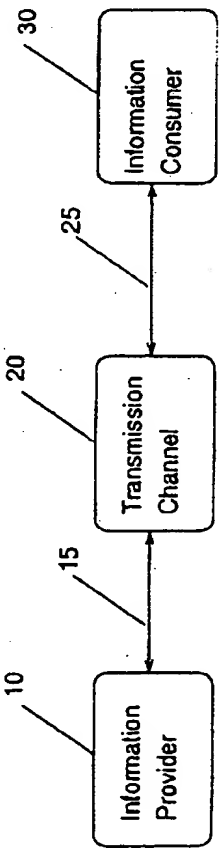

Figure 1

EP 0 644 474 A1

Brief Description of the Drawings

FIG. 1 is a model of information dissemination.
FIG. 2 illustrates sample nonuniformities on a storage medium.
FIG. 3 shows a selected list of nonuniformities on the storage medium as in FIG. 2.
FIG. 4 illustrates sample nonuniformities on another storage medium.
FIG. 5 shows the nonuniformities pattern from a bit by bit copying of the nonuniformities from the storage medium in FIG. 2 to that in FIG. 4.
FIG. 6A shows the steps an information provider prepares a distribution package in accordance to the preferred embodiment of the present invention.
FIG. 6B illustrates the flow diagram of the list generating program (LGP) used in the preferred embodiment of the present invention.
FIG. 6C illustrates the flow diagram of the signature generating program (SGP) used in the preferred embodiment of the present invention.
FIG. 7A illustrates the steps an information consumer accesses and uses the information from the distribution package prepared in FIGS. 6A - 6C.
FIG. 7B illustrates the flow diagram of the signature verification program (SVP) used in the preferred embodiment of the present invention.

Detailed Description of the Invention

A method and apparatus for utilizing medium nonuniformities to prevent the unauthorized duplication and use of digital information is described. In the following description, numerous specific details are set forth such as bit pattern and program steps, etc. in order to provide a thorough understanding of the present invention. It will be obvious to one skilled in the art that the present invention may be practised without these specific details. In other instances, well-known steps such as those involved with encryption and decryption of data are not shown in order not to obscure the present invention.

Notation and Nomenclature

The detailed description with respect to the copy protection scheme using medium signature is presented partially in terms of algorithm and symbolic representation upon operation on data bits within the computer memory. These algorithmic descriptions and representations are the means used by those skilled in the art of data processing to most effectively convey the substance of their work to others skilled in the art.

An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those require physical manipulation of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated. In this case, the physical quantities are voltage signals which correspond to the information being distributed. It proves convenient at times, principally for reason of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

Further, the manipulations performed are often referred to in terms such as adding or comparing, which are commonly associated with the mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable. In most cases, in any of the operations described herein which form part of the present invention, the operations are machine operations. Useful machines for performing the operations of the present invention include general purpose digital computers or similar devices such as digital signal processors. In all cases, it should be borne in mind that there is a distinction between the method operation in operating a computer or other apparatus and the method of computation itself. The present invention relates to method steps for preventing unauthorized use of distributed information via medium signature to generate other desired physical signals.

The present invention also relates to an apparatus for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general purpose computer as selectively activated or reconfigured by a computer program stored in the computer. The algorithms presented herein are not inherently related to any particular computer or other apparatus. In particular, various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct specialized apparatus such as digital signal processor to perform the required method steps. The required structure for a variety of these machines would appear from the description given below.

niformities of the medium. Typically, an NDP reads a given location on a storage medium, tests whether there are any nonuniformities due to the manufacturing process. These nonuniformities manifest themselves in many ways. The NDP returns a value of a location as either "good" or "bad". In general, a "bad" location is one which cannot be used for storing a chosen bit of information. Some form of NDP are used in MS-DOS® Format Command and Norton Utilities®. MS-DOS is a registered trademark of Microsoft Corporation and Norton Utilities is a registered trademark of Peter Norton.

The output from the NDP in step 60 is provided as input to step 70 where a selected list is generated by a list generating program (LGP). FIG. 6B is a flow diagram of the LGP used in the preferred embodiment of the present invention. In step 65 an integer "k" is chosen based on the characteristics of the storage medium e.g., type, capacity or otherwise. The LGP then examines the output from the NDP in step 66. Thereafter "k" elements from the nonuniformities are selected at random. At the same time, "k" elements of the uniform bits which are not on the nonuniformities list are also selected at random in step 67. The two chosen lists are permuted randomly in step 69 before it is outputted as the selected list in step 71. The LGP also supplies the attributes of the locations chosen.

Referring again to FIG. 6A, the selected list from LGP in step 70 is furnished as input to step 80 where a signature generating program (SGP) applies a pre-determined function to the selected list to derive a signature for the storage medium in question. FIG. 6C is a flow diagram of the SGP used in the preferred embodiment of the present invention. As mentioned in the preceding paragraph, the output from the LGP, the selected list, is supplied as input to the SGP in step 81. Here, the SGP fetches some pre-determined attributes of the elements from the storage medium. Next, the SGP applies a pre-determined function to the list with the attributes in step 83. Finally, in step 85 the result of the manipulation by the pre-determined function in step 83, i.e. the signature, is supplied as input to step 90 in FIG. 6A. It should be understood by one skilled in the art that the function utilized by the SGP could be a mathematical or some other pre-determined manipulation.

In FIG 6A, together with the signature of the storage medium, the present invention reads the storage medium's identification (DID-S) in step 90 in order to generate a key for encrypting the DI and/or SI in step 100. Here, the encryption key is generated by a encryption key generation program (EKGP). The details of EKGP depends on the particular encryption/decryption (EP/DP) scheme employed. In general, EKGP applies a predetermined function or manipulation to the medium signature to generate a string to the key specification of the EP/DP scheme used. EP and DP will be described further below. Next, the DI is read in step 110 and encrypted with the key generated in step 100 using a EP in step 120. The output of step 120 is the encrypted distributed information (EDI). The EP/DP can be any of the known methods of encryption and decryption. One such example is DES. See D.E.R. Denning, *Cryptography and Data Security*, Addision-Wesley, Reading, MA, 1983. In step 130, the information provider decides whether to put the EDI and SI in one or more distribution medium. Furthermore, the information provider decides whether to encrypt any of the SI. In step 140, the distribution package is then send out to the information consumer.

2. Access of information

FIGS 7A-B illustrates the manner in which the information consumer accesses and uses the information contained in the distribution package prepared in the section above. In FIG. 7 the information consumer reads in the file containing the selected list (SLF) from the distribution medium in step 150. The output from step 150 is used as an input to step 160 where the SGP is employed to generate the signature for the storage medium. Next, in step 170 the signature of the distribution medium is verified. In particular, when a storage medium is presented to a read/write peripheral, a program called signature verification program (SVP) is invoked. The SVP checks whether the signature of the medium is identical to the signature indicated in the distribution package. Referring to FIG. 7B, in step 171 the SVP reads the signature S_m from the distribution medium. The SVP then relies on NDP, LDP and SGP to generate the signature S_g of the distribution medium in step 173. The outputs of step 171 and 173 are compared in step 175. If there is no match, then a condition of incorrect signature is indicated in step 177. There are two possibilities for the incorrect signature: (1) a read/write peripheral fails to transfer the nonuniformities from the distribution medium to a copied medium, or (2) the storage medium is a copied or unauthorized medium. Both outcomes are detected by the SVP in step 175. It follows that an evade program is invoked in step 180 to halt the program altogether.

Assuming that there is a match of the signatures in step 175, then the present invention reads the device ID (DID-R) from the information consumer's device and from the designated storage device (DID-S) as shown in step 190 of FIG. 7A. Next, the ID of the designated device is authenticated in step 200 by the device verification program DVP. The DID-R from the information consumer's device is compared with the stored DID-S for the designated device. If there is no match, an evade program is enabled as an unauthorized device is found in step 210. Otherwise, the positive matching of the device IDs in step 200 activates the decryption key gen-

10. The method as defined in claim 7, wherein said signature is a function of a list of said nonuniformities, uniformities and their attributes.

11. The method as defined in claim 10, wherein said list may be a subset of all of said nonuniformities, uniformities and their attributes.

12. The method as defined in claim 11, wherein said subset may be arbitrarily selected.

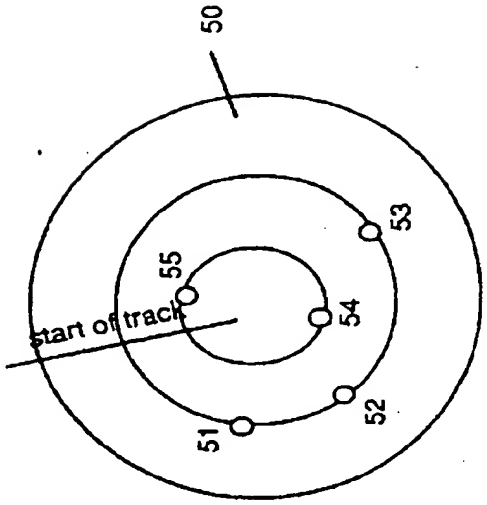

Figure 4.

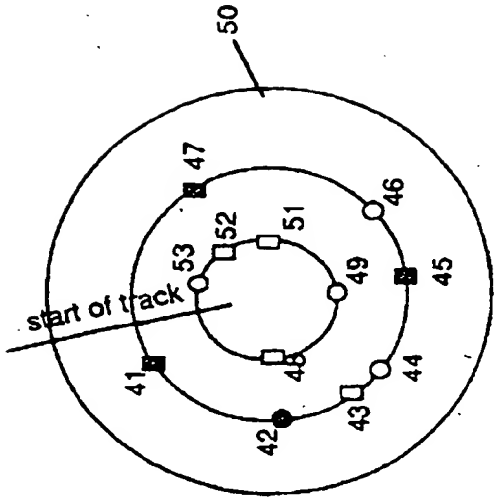

Figure 5.

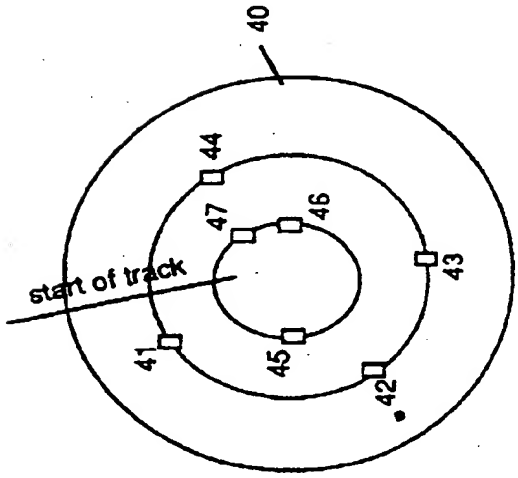

Figure 2.

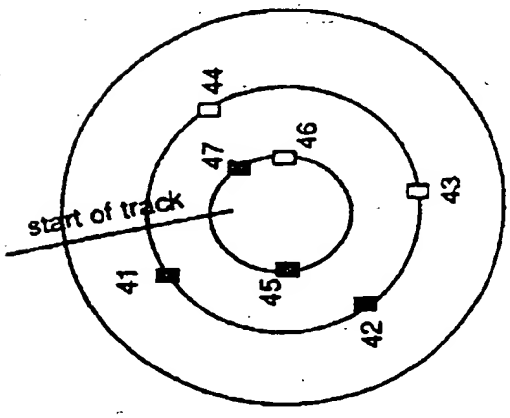

Figure 3.

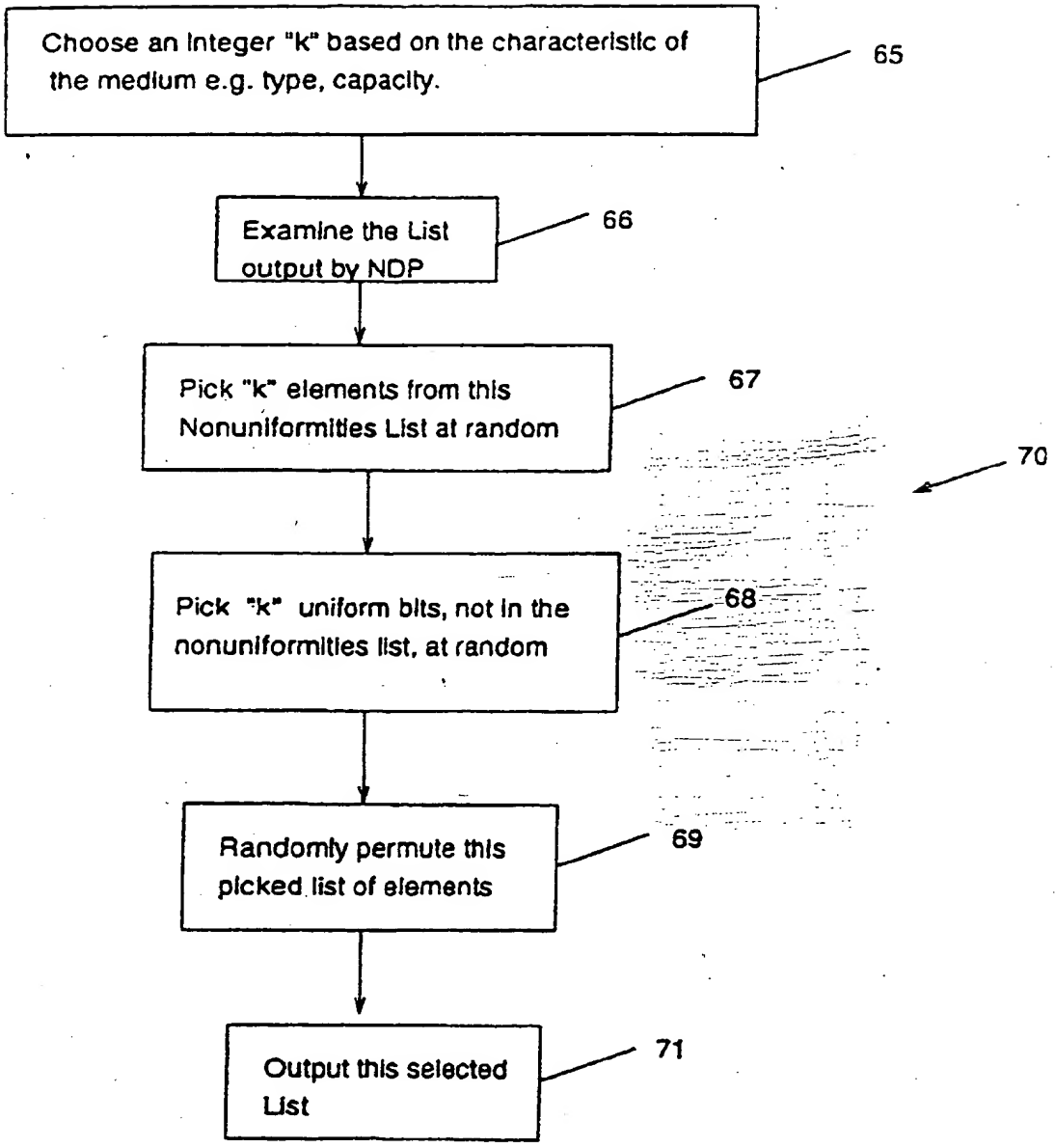

Figure 6B

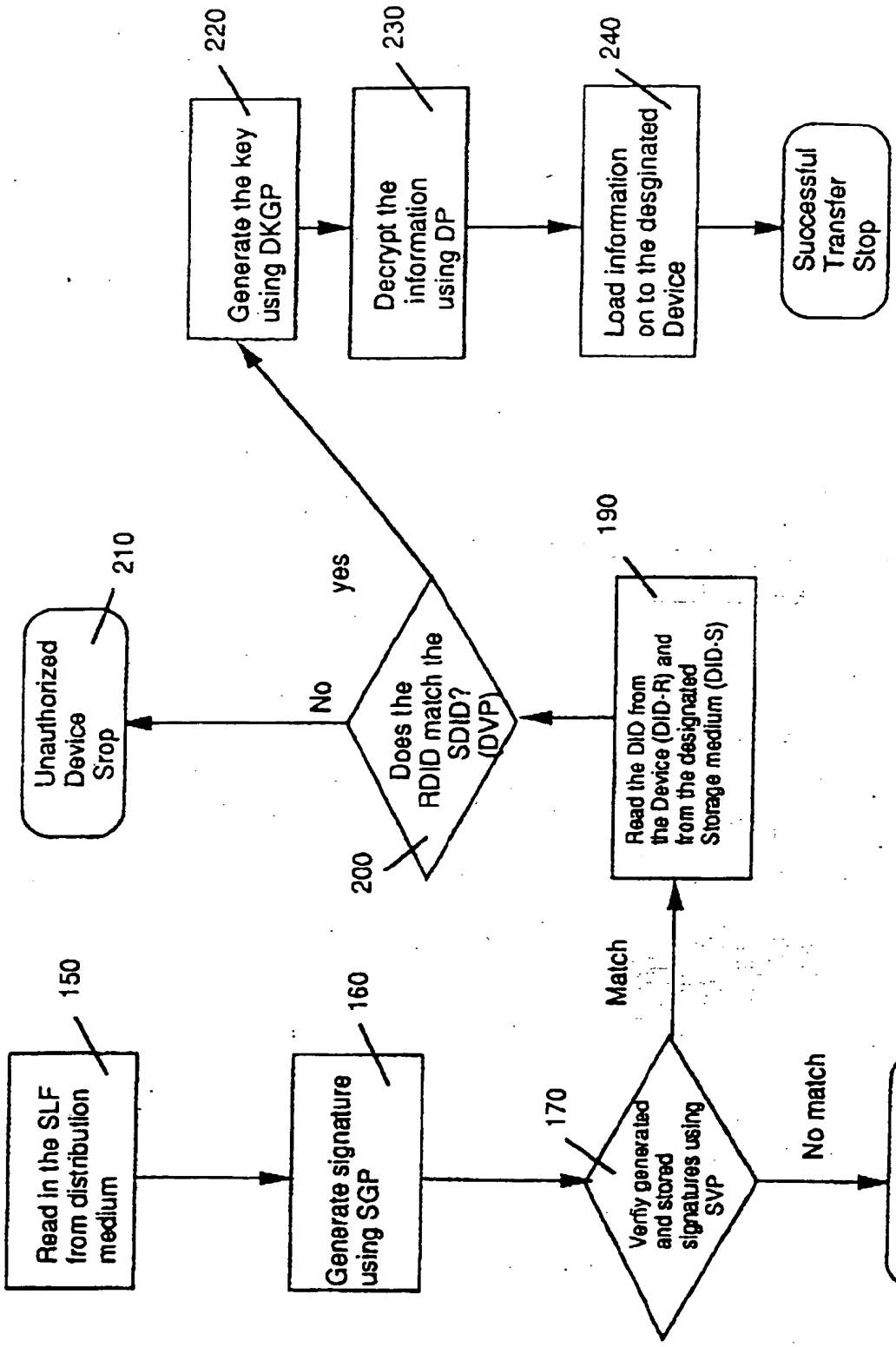

Figure 7A

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 30 6679

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	COMPUTER TECHNOLOGY REVIEW, no.3, April 1984, LOS ANGELES US page 239 W. BROTBY 'DISK FINGERPRINTING STOPS SOFTWARE PIRACY'	1	G06F1/00 G11B20/00
Y	* page 239, right column, line 22 - line 34 *	7	
A		2-6,8-12	

Y	IBM TECHNICAL DISCLOSURE BULLETIN., vol.14, no.11, April 1972, NEW YORK US page 3531 LENGYEL ET AL 'COMPUTER PROGRAM PROTECTION' * page 3531, line 7 - line 12 *	7	

A	GB-A-2 219 421 (PITNEY BOWES INC) * page 5, line 7 - page 6, line 4 * * page 8, line 3 - page 15, line 7; figure 15 *	1-12	
	-----		TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			G06F G11B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 December 1994	MOENS, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)